Email:support@f-response.com
Website:www.f-response.com
Phone: 1-800-317-5497

Best Practices: Implementing Large Scale Collections with F-Response

Note: This guide assumes you have familiarity with F-Response Enterprise or Consultant Edition. For more information, please reference the F-Response User Manual, individual Mission Guides, or the training videos on the F-Response Website.

F-Response and large scale collections

F-Response actually began as a software tool specifically designed to allow our consultants to perform large distributed investigations, collections, and incident response with the tools and techniques they had accumulated over the years. We built F-Response to make large (and small) scale network based collections and investigations easier, more flexible, faster, and within reach of just about any project budget.

Scope and Planning

Prior to commencing any large scale collection engagement it is critical to establish the scope and parameters of the exercise. You will want to ask the important questions, such as:

- What is the scope of the data to be collected?
  - Is the client interested in full disk images, logical files, a combination?
  - Is there a defined list of custodians, by machine, by employee, by IP Address?
  - Where are the custodians located? Local LAN, WAN, or Remote VPN?
  - If we are collecting full disk images, how large is the average custodian hard drive? Are we collecting unallocated space, or only allocated files?
  - If we are collecting logical files, are they identified by location, or by name, size, or extension? What criteria will be used to identify the files and is it subject to interpretation?
  - Is full disk encryption in use on the custodian machines? Can we access the device un-encrypted by connecting to the logical volume? Are there filter drivers or overlays that will allow us to access the encrypted disk natively?
  - Is this a covert engagement? Should the custodian be unaware of the collection effort?

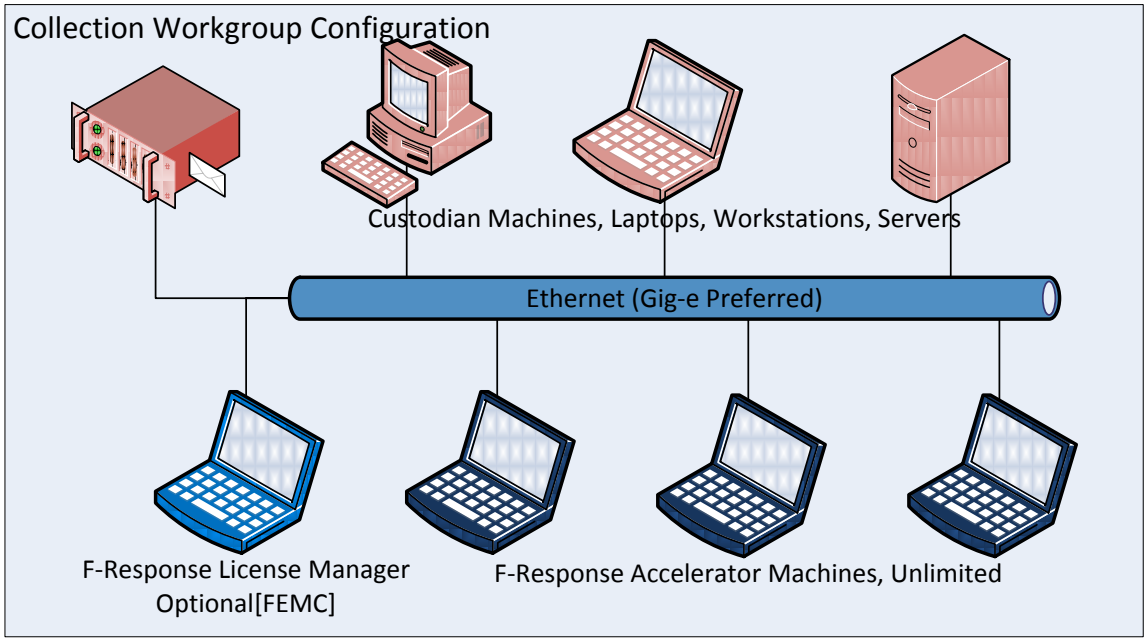
Email:support@f-response.com
Website:www.f-response.com
Phone: 1-800-317-5497

- Is there a preferred final delivery format? What post processing will be required?

Preparing Your Collection Workgroup

First we'll want to define the collection workgroup. We recommend leveraging the unlimited licensing model of F-Response Consultant, Enterprise, and even Consultant + Covert to engage multiple collection machines in a small workgroup configuration.

In this model we would have one machine in the workgroup acting as our F-Response License Manager/Master, and all other collection machines using the F-Response Accelerator. In order to leverage this model you will need to install F-Response Consultant edition or higher on all Accelerator machines. No additional license dongle or license is required. The following diagram outlines the recommended configuration:



Next, we recommend you make certain all your designated collection machines (laptops, workstations, or even virtual machines) are running Windows 7 as their operating system. Alternately, if you are performing your collections using Linux, we recommend a modern Linux distribution with the Open-iSCSI[1] tools installed.

[1] Open-iSCSI tools are available for almost all major Linux Distributions. More information can be found at www.open-iscsi.org

Email:support@f-response.com
Website:www.f-response.com
Phone: 1-800-317-5497

In addition, if possible we recommend Gigabit Ethernet, the speed and performance afforded by Gigabit Ethernet is definitely worth the investment in additional local workgroup switches or networking equipment.

Lastly, with regards to imaging software, we have found that not all imaging products perform the same, in our tests X-Ways Imager and X-Ways Forensics are exceptionally fast when paired with F-Response and Windows 7. While the X-Ways Imager product is not free, it is reasonably priced and can readily be factored into the cost of the engagement.

The above recommendations should go a long way in optimizing your full disk imaging experience. However, should your collection objectives call for logical file collection you have much more flexibility. There are a number of options you can consider including:

- Leveraging the F-Response Flexdisk API and Powershell scripts to collect individual files from custodian machines.[2]
- Use individual forensics applications to create logical containers of required content, either by scripting or manually.

Custodian Machines/Network

Once the scope of the collection effort is defined, we can look at the environment to determine the challenge to acquisition.

Machines in a remote office

When looking at collecting a remote machine we need to consider the speed of the WAN link and the size of the data to be collected. It may make more sense to look at setting up a collection machine in the remote location to perform the collection and have the results shipped back (If security is a concern, the data can always be collected to an encrypted drive). By making use of USB-Over-Ethernet [3]the licensing dongles for any of your forensics tools can be forwarded to the remote collection machine giving you the option of not having to ship any equipment to the remote site. In addition, since the F-Response Accelerator can used on an unlimited number of collection machines, you can readily configure an Accelerator much closer to the custodian machine, ie on the same local LAN segment as the custodian.

[2] Automating Large Collections with Flexdisk/Powershell (F-Response Website)
[3] USB-Over-Ethernet is available from www.usb-over-ethernet.com.

Email:support@f-response.com
Website:www.f-response.com
Phone: 1-800-317-5497

Firewalls/AV

Firewalls can sometimes interfere with F-Response communication. Thankfully in a large environment, the firewall is usually centrally managed through policy and exceptions can be made for the required F-Response ports: 3260, 3261, and 5681. If possible, work with the Network Administrator to allow for F-Response to run on these ports, or temporarily disable the local firewall on the target machines.

Anti-Virus(A/V)

AV software can interfere with communications on the remote target machine. It may not only prohibit communication, but may slow down the collection process by interfering with each read command during the imaging process. Again, work with the local Administrator to make exceptions/temporarily disable AV on the target machine.

Active Directory

If your custodian machines are part of an Active Directory we recommend the following modifications be made to maximize uptime and performance. All of these recommendations can be accomplished by creating a separate Organizational Unit ("OU") within the domain and applying the policy changes to that OU.

- Where possible disable the automatic application of Windows Updates.
- Where possible alter the power policy to disable sleep, poweroff, or any other low power state.
- Set firewall exceptions either based on port, or based on the IP/hostname of the collection machines/workgroup.
- Temporarily disable Anti-Virus software.

In addition when working with Active Directory managed environments you'll want to review the domains and trusts. Any account you provision to deploy F-Response (or deploy via MSI) must have sufficient trust to operate between domains within the Active Directory.

Backup Intervals and Maintenance

Additional consideration should also be given to backup windows and standard system maintenance.

- Are any custodian systems (servers or workstations) part of a backup rotation that would make them unavailable for a period of time?

Email:support@f-response.com
Website:www.f-response.com
Phone: 1-800-317-5497

- Is there a general system maintenance window where custodian systems might be rebooted? Are administrators of those maintenance windows aware of your operations such that impacted custodian systems will not be affected?

Laptops

Are the target machines local laptop users? Are they aware of the collection? If the target employee is aware of the collection we can simply ask they leave their machine connected to the network until the process is complete.

If the laptop must be collected in a covert manner, there is a bit more planning involved. We will want to look at using a tool for collection that will allow us to reconnect and continue imaging should the user disconnect from the network. Not all Forensic imaging products allow for the restart of a incomplete image, you will want to review your tool selection independently.

Deployment

Depending on the version of F-Response you are using you'll have the following deployment options available to get F-Response running on the custodian machines:

- F-Response Enterprise
  - The F-Response Enterprise Management Console (FEMC)
    - You will need valid credentials on the network, either Domain Administrator, or Credentials with permission to access the remote computer from the network[4].
  - The F-Response Enterprise Scriptable COM Object
    - You will need valid credentials on the network, either Domain Administrator, or Credentials with permission to access the remote computer from the network.
  - F-Response Enterprise MSI Installer
    - You will need valid credentials as indicated above, alternatively the MSI can be provided to an administrator to be applied to target machines.
- F-Response Consultant + Covert
  - F-Response Covert Console (single covert target at any given time)

[4] Additional guidelines for Active Directory permissions is available on our website at https://www.f-response.com/index.php?option=com_content&view=article&id=357:using-active-directory-to-delegate-f-response-ee-duties&catid=34:blog-posts

Email:support@f-response.com
Website:www.f-response.com
Phone: 1-800-317-5497

        - Both the FEMC and FEMC COM object options outlined above will work for deployment.
    - F-Response Consultant edition executable (GUI on target machine, unlimited usage)
        - The F-Response Consultant Edition executable (f-response-ce.exe) must be executed on the target machine with administrative privileges.
- F-Response Consultant
    - F-Response Consultant edition executable (GUI on target machine, unlimited usage)
        - The F-Response Consultant Edition executable (f-response-ce.exe) must be executed on the target machine with administrative privileges.

Various Operating Systems

What Operating Systems (OSs) are running on the machines to be collected? In addition it will be important to know what must be collected on non-Windows systems, as drives and partitions may look very different than their Windows counterparts. F-Response Enterprise, Consultant + Covert, and Consultant Edition support over ten major operating system environments:

Windows Includes Windows 2000, XP, 2003, Vista, 2008,7 & 8, 32 and 64bit, Physical memory only supported on 32bit and 64bit Windows
Apple OSX Includes OSX 10.3,10.4,10.5,10.6, 10.7, 10.8 Universal Binary
Linux includes most Linux distributions build on Glibc 2.3.5 and higher
Solaris includes Solaris 8, 9, & 10 on SPARC and **OpenSolaris, Oracle Solaris** on Intel
IBM AIX includes AIX 5.1,5.2,5.3,6.1 on the Power processor
HPUX includes HP_UX11iv2,11iv3 on the Itanium processor
FreeBSD includes FreeBSD 7 on the Intel/i386 processor
SCO includes SCO OpenServer 6 and Unixware 7 on the Intel/i386 processor

Divide and Conquer

In addition to all the recommendations provided above, we also recommend grouping the custodian collection activities into manageable sized logical units wherever possible. These logical units can be re-run if necessary, and greatly reduce the exposure to unforeseen environmental issues (emergency power loss, network interruption, etc).